

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-173

### Vulnerability Summary for the Week of June 15, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
elvinbts -- elvinbts	SQL injection vulnerability in close_bug.php in Elvin before 1.2.1 allows remote attackers to execute arbitrary SQL commands via the title (aka subject) field.	2009-06-19	7.5	<a href="#">CVE-2009-2128 CONFIRM</a>	
angrydonuts -- nodequeue	Nodequeue 5.x before 5.x-2.7 and 6.x before 6.x-2.2, a module for Drupal, does not properly restrict access when displaying node titles, which has unknown impact and attack vectors.	2009-06-16	7.5	<a href="#">CVE-2009-2075 BID CONFIRM CONFIRM CONFIRM</a>	
apple -- iphone_os	The MPEG-4 video codec in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 allows remote attackers to cause a denial of service (device reset) via a crafted MPEG-4 video file that triggers an "input validation issue."	2009-06-19	7.1	<a href="#">CVE-2009-0959 CONFIRM APPLE</a>	
apple -- iphone_os	The Telephony component in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 allows remote attackers to cause a denial of service (device reset) via a crafted ICMP echo request, which triggers an assertion error related to a "logic issue."	2009-06-19	7.8	<a href="#">CVE-2009-1683 CONFIRM APPLE</a>	
	WebKit in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 allows			<a href="#">CVE-2009-</a>	

apple -- iphone_os	remote attackers to cause a denial of service (device reset) via a web page containing an HTMLSelectElement object with a large length attribute.	2009-06-19	7.1	<a href="#">1692 CONFIRM APPLE</a>
com_jumi -- com_jumi	SQL injection vulnerability in the Jumi (com_jumi) component 2.0.3 and possibly other versions for Joomla allows remote attackers to execute arbitrary SQL commands via the fileid parameter to index.php.	2009-06-17	7.5	<a href="#">CVE-2009-2102 BID MILWORM SECUNIA</a>
creative_web_solutions -- multi-level_cms	SQL injection vulnerability in insidepage.php in Creative Web Solutions Multi-Level CMS 1.21 allows remote attackers to execute arbitrary SQL commands via the catid parameter. NOTE: some of these details are obtained from third party information.	2009-06-16	7.5	<a href="#">CVE-2009-2082 BID SECUNIA MISC OSVDB</a>
daan_sprenkels -- fretsweb	Multiple SQL injection vulnerabilities in FretsWeb 1.2 allow remote attackers to execute arbitrary SQL commands via the (1) name parameter to player.php and the (2) hash parameter to song.php.	2009-06-18	7.5	<a href="#">CVE-2009-2113 CONFIRM</a>
david_degner -- phpcollegeexchange	SQL injection vulnerability in house/listing_view.php in phpCollegeExchange 0.1.5c allows remote attackers to execute arbitrary SQL commands via the itemnr parameter.	2009-06-17	7.5	<a href="#">CVE-2009-2096 MILWORM SECUNIA</a>
dxstudio -- dx_studio_player	Worldweaver DX Studio Player 3.0.29.0, 3.0.22.0, 3.0.12.0, and probably other versions before 3.0.29.1, when used as a plug-in for Firefox, does not restrict access to the shell.execute JavaScript API method, which allows remote attackers to execute arbitrary commands via a .dxstudio file that invokes this method.	2009-06-16	7.5	<a href="#">CVE-2009-2011 VUPEN BID</a>
elvinbts -- elvinbts	Multiple SQL injection vulnerabilities in Elvin 1.2.0 allow remote attackers to execute arbitrary SQL commands via the (1) inUser (aka Username) and (2) inPass (aka Password) parameters to (a) inc/login.ei, reachable through login.php; and the (3) id parameter to (b) show_bug.php and (c) show_activity.php.	2009-06-19	7.5	<a href="#">CVE-2009-2123 MILWORM SECUNIA</a>
elvinbts -- elvinbts	Directory traversal vulnerability in page.php in Elvin 1.2.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the id parameter.	2009-06-19	7.5	<a href="#">CVE-2009-2124 MILWORM SECUNIA</a>
frank-karau -- phpfk	Directory traversal vulnerability in include/page_bottom.php in phpFK 7.03 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the _FORUM[settings_design_style] parameter.	2009-06-18	7.5	<a href="#">CVE-2009-2112 MILWORM</a>
geekbill -- open_biller	SQL injection vulnerability in index.php in Open Biller 0.1 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-06-12	7.5	<a href="#">CVE-2009-2036 BUGTRAQ MILWORM OSVDB</a>
ijoomla -- com_rssfeeder	SQL injection vulnerability in the iJoomla RSS Feeder (com_ijoomla_rss) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the cat parameter in an xml action to index.php.	2009-06-17	7.5	<a href="#">CVE-2009-2099 BID MILWORM SECUNIA</a>
				<a href="#">CVE-2009-</a>

jnmsolutions -- db_top_sites	Multiple directory traversal vulnerabilities in DB Top Sites 1.0, when magic_quotes_gpc is disabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the u parameter to (1) full.php, (2) index.php, and (3) contact.php.	2009-06-18	7.6	2110 XF MILWORM SECUNIA OSVDB OSVDB OSVDB
jnmsolutions -- db_top_sites	Static code injection vulnerability in add_reg.php in DB Top Sites 1.0 allows remote attackers to inject arbitrary PHP code via a crafted (1) url and (2) location parameter.	2009-06-18	10.0	CVE-2009-2111 XF MILWORM SECUNIA OSVDB
kasper_skrhj -- references_database	SQL injection vulnerability in the References database (t3references) extension 0.1.1 and earlier allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-06-17	7.5	CVE-2009-2105 CONFIRM CONFIRM
linux -- kernel linux -- kernel linux -- linux_kernel	Buffer overflow in the RTL8169 NIC driver (drivers/net/r8169.c) in the Linux kernel before 2.6.30 allows remote attackers to cause a denial of service (kernel memory corruption and crash) via a long packet.	2009-06-16	7.8	CVE-2009-1389 CONFIRM XF MLIST SECUNIA MLIST MLIST CONFIRM
llnl -- slurm	Simple Linux Utility for Resource Management (SLURM) 1.2 and 1.3 before 1.3.14 does not properly set supplementary groups before invoking (1) sbcast from the slurmd daemon or (2) trigger from the slurmctld daemon, which might allow local SLURM users to modify files and gain privileges.	2009-06-16	7.2	CVE-2009-2084 XF XF VUPEN BID DEBIAN
micheal_glazer -- phportal	SQL injection vulnerability in topicler.php in phPortal 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-06-17	7.5	CVE-2009-2098 BID MILWORM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The browser engine in Mozilla Firefox 3 before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsEventManager::GetContentState and nsNativeTheme::CheckBooleanAttr; (2) UnhookTextRunFromFrames and ClearAllTextRunReferences; (3) nsTextFrame::ClearTextRun; (4) IsPercentageAware; (5) PL_DHashTableFinish; (6) nsListBoxBodyFrame::GetNextItemBox; (7) AtomTableClearEntry, related to the atom table, DOM mutation events, and Unicode surrogates; (8) nsHTMLEditor::HideResizers; and (9) nsWindow::SetCursor, related to changing the cursor; and other vectors.	2009-06-12	9.3	CVE-2009-1392 REDHAT VUPEN SECTRACK REDHAT
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute	2009-06-12	9.3	CVE-2009-1832 REDHAT VUPEN

mozilla -- thunderbird	arbitrary code via vectors involving "double frame construction."			VUPEN SECTRACK
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The JavaScript engine in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) js_LeaveSharpObject, (2) ParseXMLSource, and (3) a certain assertion in jsinterp.c; and other vectors.	2009-06-12	9.3	CVE-2009-1833 VUPEN SECTRACK
mozilla -- firefox	Race condition in the NPObjWrapper_NewResolve function in modules/plugin/base/src/nsJSNPRuntime.cpp in xul.dll in Mozilla Firefox 3 before 3.0.11 might allow remote attackers to execute arbitrary code via a page transition during Java applet loading, related to a use-after-free vulnerability for memory associated with a destroyed Java object.	2009-06-12	9.3	CVE-2009-1837 FEDORA FEDORA REDHAT CONFIRM CONFIRM VUPEN SECTRACK BID BID BUGTRAQ CONFIRM MISC SECUNIA SECUNIA SECUNIA
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The garbage-collection implementation in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 sets an element's owner document to null in unspecified circumstances, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted event handler, related to an incorrect context for this event handler.	2009-06-12	9.3	CVE-2009-1838 VUPEN BID
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.11, Thunderbird, and SeaMonkey do not check content policy before loading a script file into a XUL document, which allows remote attackers to bypass intended access restrictions via a crafted HTML document, as demonstrated by a "web bug" in an e-mail message, or web script or an advertisement in a web page.	2009-06-12	9.3	CVE-2009-1840 VUPEN BID
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	js/src/xpconnect/src/xpcwrappedjsclass.cpp in Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 allows remote attackers to execute arbitrary web script with the privileges of a chrome object, as demonstrated by the browser sidebar and the FeedWriter.	2009-06-12	9.3	CVE-2009-1841 VUPEN
mrcgiguy -- the_ticket_system	admin.php in MRCGIGUY The Ticket System 2.0 does not properly restrict access, which allows remote attackers to (1) obtain sensitive configuration information via the editconfig action or (2) change the administrator's password via the id parameter in an editop action.	2009-06-16	7.5	CVE-2009-2080 XF MILWORM SECUNIA
paolo_palmonari -- photoracer_plugin_for_wordpress	SQL injection vulnerability in viewing.php in the Paolo Palmonari Photoracer plugin 1.0 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-06-19	7.5	CVE-2009-2122 XF BID MILWORM SECUNIA

phportal -- phportal	uye_paneli.php in phPortal 1.0 allows remote attackers to bypass authentication and obtain administrative access by setting the kulladi cookie to a valid username.	2009-06-18	7.5	CVE-2009-2117 MILWORM
projektseminar_proservice_wwu -- virtual_civil_services	SQL injection vulnerability in the Virtual Civil Services (civserv) extension 4.3.2 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-06-17	7.5	CVE-2009-2106 CONFIRM CONFIRM SECUNIA
steve_grundell -- frontend_mp3_player	SQL injection vulnerability in the Frontend MP3 Player (fe_mp3player) 0.2.3 and earlier extension for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-06-17	7.5	CVE-2009-2103 CONFIRM CONFIRM SECUNIA
sun -- jre	The Aqua Look and Feel for Java implementation in Java 1.5 on Mac OS X 10.5 allows remote attackers to execute arbitrary code via a call to the undocumented apple.laf.CColourUIResource constructor with a crafted value in the first argument, which is dereferenced as a pointer.	2009-06-16	7.5	CVE-2009-1719 BID BID CONFIRM APPLE
zokisoft -- zoki_catalog	SQL injection vulnerability in system/application/controllers/catalog.php in Zoki Soft Zoki Catalog (aka Smart Catalog) allows remote attackers to execute arbitrary SQL commands via the search_text parameter. NOTE: some of these details are obtained from third party information.	2009-06-17	7.5	CVE-2009-2097 BUGTRAQ MISC SECUNIA

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activecollab -- activecollab	Cross-site scripting (XSS) vulnerability in A51 D.O.O. activeCollab 0.7.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2009-1772.	2009-06-12	4.3	CVE-2009-2041 OSVDB JVN
angrydonuts -- views	Drupal 6.x before 6.x-2.6, a module for Drupal, allows remote authenticated users to bypass access restrictions and (1) read unpublished content from anonymous users when a view is already configured to display the content, and (2) read private content in generated queries.	2009-06-16	4.0	CVE-2009-2077 BID CONFIRM CONFIRM
apache -- tomcat	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalizes the target pathname before filtering the query string when using the RequestDispatcher method, which allows remote attackers to bypass intended access restrictions and conduct directory traversal attacks via .. (dot dot) sequences and the WEB-INF directory in a Request.	2009-06-16	5.0	CVE-2008-5515 VUPEN BID BUGTRAQ BUGTRAQ CONFIRM CONFIRM CONFIRM JVN
	Apple Safari before 3.2.2 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT	2009-06-16		CVE-2009-2070

apple -- safari	response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.	2009-06-15	6.8	<a href="#">CVE-2009-1550</a> MISC MISC
apple -- safari	Apple Safari before 3.2.2 processes a 3xx HTTP CONNECT response before a successful SSL handshake, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying this CONNECT response to specify a 302 redirect to an arbitrary https web site.	2009-06-15	6.8	<a href="#">CVE-2009-2062</a> MISC MISC
apple -- safari	Apple Safari detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."	2009-06-15	6.8	<a href="#">CVE-2009-2066</a> MISC MISC
apple -- safari	Apple Safari does not require a cached certificate before displaying a lock icon for an https web site, which allows man-in-the-middle attackers to spoof an arbitrary https site by sending the browser a crafted (1) 4xx or (2) 5xx CONNECT response page for an https request sent through a proxy server.	2009-06-15	5.4	<a href="#">CVE-2009-2072</a> MISC MISC
apple -- iphone_os	Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 stores an exception for a hostname when the user accepts an untrusted Exchange server certificate, which causes it to be accepted without prompting in future usage and allows remote Exchange servers to obtain sensitive information such as credentials.	2009-06-19	4.3	<a href="#">CVE-2009-0958</a> CONFIRM APPLE
apple -- iphone_os	The Mail component in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 does not provide an option to disable remote image loading in HTML email, which allows remote attackers to determine when an e-mail was read and the device address via an HTML email containing an image URL.	2009-06-19	5.0	<a href="#">CVE-2009-0960</a> CONFIRM APPLE
apple -- iphone_os	The Mail component in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 dismisses the call approval dialog when another alert appears, which might allow remote attackers to force the iPhone to place a call without user approval by causing an application to trigger an alert.	2009-06-19	5.0	<a href="#">CVE-2009-0961</a> CONFIRM APPLE
apple -- iphone_os	The Profiles component in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1, when installing a configuration profile, can replace the password policy from Exchange ActiveSync with a weaker password policy, which allows physically proximate attackers to bypass the intended policy.	2009-06-19	4.6	<a href="#">CVE-2009-1679</a> CONFIRM APPLE
	The message engine in CA ARCserve Backup r12.0 and r12.0 SP1 for Windows allows remote			<a href="#">CVE-2009-2000</a>

ca -- areserve_backup	attackers to cause a denial of service (crash) via (1) an invalid ox13 message, which is not properly handled in the ASCORE module, or (2) a ox3B message with invalid stub data that triggers an RPC marshalling error.	2009-06-16	5.0	CVE-2009-1761 CONFIRM CONFIRM
castro_xl -- torrentvolve	Directory traversal vulnerability in archive.php in TorrentVolve 1.4, when register_globals is enabled, allows remote attackers to delete arbitrary files via a .. (dot dot) in the deleteTorrent parameter.	2009-06-17	6.8	CVE-2009-2101 XF MILWoRM
daan_sprenkels -- fretsweb	Multiple directory traversal vulnerabilities in FretsWeb 1.2 allow remote attackers to read arbitrary files via directory traversal sequences in the (1) language parameter to charts.php and the (2) fretsweb_language cookie parameter to unspecified vectors, possibly related to admin/common.php.	2009-06-18	5.0	CVE-2009-2109 MILWoRM SECUNIA
drupal -- views	Cross-site scripting (XSS) vulnerability in Views 6.x before 6.x-2.6, a module for Drupal, allows remote authenticated users to inject arbitrary web script or HTML via (1) exposed filters in the Views UI administrative interface and in the (2) view name parameter in the define custom views feature. NOTE: vector 2 is only exploitable by users with administer views permissions.	2009-06-16	4.3	CVE-2009-2076 CONFIRM CONFIRM
elvinbts -- elvinbts	delete_bug.php in Elvin before 1.2.1 does not require administrative privileges, which allows remote authenticated users to bypass intended access restrictions and delete arbitrary bugs.	2009-06-19	4.0	CVE-2009-2125 CONFIRM
elvinbts -- elvinbts	Cross-site scripting (XSS) vulnerability in close_bug.php in Elvin before 1.2.1 allows remote attackers to inject arbitrary web script or HTML via the title (aka subject) field.	2009-06-19	4.3	CVE-2009-2126 CONFIRM
elvinbts -- elvinbts	Cross-site scripting (XSS) vulnerability in show_activity.php in Elvin 1.2.0 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2009-06-19	4.3	CVE-2009-2127 MILWoRM SECUNIA
f5 -- firepass_ssl_vp	Cross-site scripting (XSS) vulnerability in the login interface in F5 FirePass SSL VPN 5.5 through 5.5.2 and 6.0 through 6.0.3 allows remote attackers to inject arbitrary web script or HTML via a crafted password field. NOTE: some of these details are obtained from third party information.	2009-06-18	4.3	CVE-2009-2119 XF VUPEN SECTRACK BUGTRAQ
freebsd -- freebsd	Integer overflow in the pipe_build_write_buffer function (sys/kern/sys_pipe.c) in the direct write optimization feature in the pipe implementation in FreeBSD 7.1 through 7.2 and 6.3 through 6.4 allows local users to bypass virtual-to-physical address lookups and read sensitive information in memory pages via unspecified vectors.	2009-06-18	4.9	CVE-2009-1935 FREEBSD
git -- git	git-daemon in git 1.4.4.5 through 1.6.3 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a request containing extra unrecognized arguments.	2009-06-18	5.0	CVE-2009-2108 MLIST VUPEN MLIST MISC MISC

google -- chrome	src/net/http/http_transaction_winhttp.cc in Google Chrome before 1.0.154.53 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.	2009-06-15	5.8	CVE-2009-2060 MISC CONFIRM CONFIRM CONFIRM MISC MISC MISC MISC
google -- chrome	Google Chrome before 1.0.154.53 displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.	2009-06-15	6.8	CVE-2009-2071 CONFIRM CONFIRM
heine.familiedeelstra -- booktree	Multiple cross-site scripting (XSS) vulnerabilities in Booktree 5.x before 5.x-7.3 and 6.x before 6.x-1.1, a module for Drupal, allow remote attackers to inject arbitrary web script or HTML via the (1) node title and (2) node body in a tree root page.	2009-06-16	4.3	CVE-2009-2078 BID CONFIRM CONFIRM CONFIRM
irfanview -- irfanview	Integer overflow in IrfanView 4.23, when the resampling or screen fitting option is enabled, allows remote attackers to execute arbitrary code via a crafted TIFF 1 BPP image, which triggers a heap-based buffer overflow.	2009-06-18	6.8	CVE-2009-2118 BID CONFIRM
joomlapraise -- com_projectfork	Directory traversal vulnerability in the JoomlaPraise Projectfork (com_projectfork) component 2.0.10 for Joomla! allows remote attackers to read arbitrary files via directory traversal sequences in the section parameter to index.php.	2009-06-17	5.0	CVE-2009-2100 BID MILWoRM
libpng -- libpng	libpng before 1.2.37 does not properly parse 1-bit interlaced images with width values that are not divisible by 8, which causes libpng to include uninitialized bits in certain rows of a PNG file and might allow remote attackers to read portions of sensitive memory via "out-of-bounds pixels" in the file.	2009-06-12	4.3	CVE-2009-2042 VUPEN BID CONFIRM
microsoft -- ie	Microsoft Internet Explorer before 8 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.	2009-06-15	5.8	CVE-2009-2057 MISC MISC
microsoft -- internet_explorer microsoft -- pocket_internet_explorer	Microsoft Internet Explorer 8, and possibly other versions, detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable"	2009-06-15	6.8	CVE-2009-2064 MISC MISC

	(HPIHSL) pages."			
microsoft -- ie	Microsoft Internet Explorer before 8 displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.	2009-06-15	5.8	CVE-2009-2069 MISC MISC
mozilla -- firefox mozilla -- seamonkey	Visual truncation vulnerability in network/dns/src/nsIDNSService.cpp in Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 allows remote attackers to spoof the location bar via an IDN with invalid Unicode characters that are displayed as whitespace, as demonstrated by the \u115A through \u115E characters.	2009-06-12	4.3	CVE-2009-1834 VUPEN
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.11 and SeaMonkey before 1.1.17 associate local documents with external domain names located after the file:// substring in a URL, which allows user-assisted remote attackers to read arbitrary cookies via a crafted HTML document, as demonstrated by a URL with file://example.com/C:/ at the beginning.	2009-06-12	4.3	CVE-2009-1835 REDHAT VUPEN REDHAT
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.11, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.17 use the HTTP Host header to determine the context of a document provided in a non-200 CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.	2009-06-12	6.8	CVE-2009-1836 REDHAT VUPEN
mozilla -- firefox	Mozilla Firefox 3 before 3.0.11 associates an incorrect principal with a file: URL loaded through the location bar, which allows user-assisted remote attackers to bypass intended access restrictions and read files via a crafted HTML document, aka a "file-URL-to-file-URL scripting" attack.	2009-06-12	5.4	CVE-2009-1839 VUPEN BID
mozilla -- firefox	Mozilla Firefox before 3.0.10 processes a 3xx HTTP CONNECT response before a successful SSL handshake, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying this CONNECT response to specify a 302 redirect to an arbitrary https web site.	2009-06-15	6.8	CVE-2009-2061 MISC MISC
mozilla -- firefox	Mozilla Firefox 3.0.10, and possibly other versions, detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."	2009-06-15	6.8	CVE-2009-2065 MISC MISC
	PHP remote file inclusion vulnerability in			

mundi_king -- mundi_mail	template/simpledefault/admin/_masterlayout.php in Mundi Mail 0.8.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the top parameter. NOTE: when allow_url_fopen is disabled, directory traversal attacks are possible to include and execute arbitrary local files.	2009-06-17	6.8	CVE-2009-2095 MILWoRM
mutt -- mutt	Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.	2009-06-16	6.8	CVE-2009-1390 XF BID MLIST CONFIRM
opera -- opera_browser	Opera, possibly before 9.25, uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.	2009-06-15	6.8	CVE-2009-2059 MISC MISC
opera -- opera	Opera, possibly before 9.25, processes a 3xx HTTP CONNECT response before a successful SSL handshake, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying this CONNECT response to specify a 302 redirect to an arbitrary https web site.	2009-06-15	6.8	CVE-2009-2063 MISC MISC
opera -- opera_browser	Opera detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."	2009-06-15	6.8	CVE-2009-2067 MISC MISC
opera -- opera	Google Chrome detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."	2009-06-15	5.8	CVE-2009-2068 MISC MISC
opera -- opera	Opera displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.	2009-06-15	6.8	CVE-2009-2070 MISC MISC
pagedowntech -- pdshoppro	Cross-site scripting (XSS) vulnerability in search.asp in PDshopPro, when downloaded before 20070308, allows remote attackers to inject arbitrary web script or HTML via the search parameter.	2009-06-12	4.3	CVE-2009-2032 SECUNIA MISC OSVDB

paul_marquess -- compress-raw-zlib_perl_module	Off-by-one error in the inflate function in Zlib.xs in Compress::Raw::Zlib Perl module before 2.017, as used in AMaViS, SpamAssassin, and possibly other products, allows context-dependent attackers to cause a denial of service (hang or crash) via a crafted zlib compressed stream that triggers a heap-based buffer overflow, as exploited in the wild by TrojanDownloader-71014 in June 2009.	2009-06-16	6.8	CVE-2009-1391 XF VUPEN BID
phpwebthings -- phpwebthings	Directory traversal vulnerability in help.php in phpWebThings 1.5.2 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the module parameter.	2009-06-16	4.3	CVE-2009-2081 MILWoRM
ricardo_alexandre_de_oliveira_staudt -- yogurt	Cross-site scripting (XSS) vulnerability in index.php in Yogurt 0.3 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	2009-06-12	4.3	CVE-2009-2033 BID MILWoRM OSVDB
ricardo_alexandre_de_oliveira_staudt -- yogurt	SQL injection vulnerability in writemessage.php in Yogurt 0.3, when register_globals is enabled, allows remote authenticated users to execute arbitrary SQL commands via the original parameter.	2009-06-12	6.0	CVE-2009-2034 BID MILWoRM OSVDB
skybluecanvas -- skybluecanvas	Multiple cross-site scripting (XSS) vulnerabilities in admin.php in SkyBlueCanvas 1.1 r237 allow remote attackers to inject arbitrary web script or HTML via the (1) mgroup, (2) mgr, (3) objtype, (4) id, and (5) dir parameters.	2009-06-18	4.3	CVE-2009-2114 XF
skybluecanvas -- skybluecanvas	Directory traversal vulnerability in admin.php in SkyBlueCanvas 1.1 r237 allows remote authenticated administrators to list directory contents via a .. (dot dot) in the dir parameter.	2009-06-18	4.0	CVE-2009-2116 BUGTRAQ
tekbase -- tekbase_all-in-one	Multiple SQL injection vulnerabilities in TekBase All-in-One 3.1 allow remote authenticated users to execute arbitrary SQL commands via the (1) ids parameter to admin.php, the (2) y parameter to members.php, and other unspecified vectors.	2009-06-18	6.5	CVE-2009-2120 MILWoRM
udo_von_eynern -- modern_guest_book_commenting_system	Cross-site scripting (XSS) vulnerability in the Modern Guestbook / Commenting System (ve_guestbook) extension 2.7.1 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-06-17	4.3	CVE-2009-2104 CONFIRM CONFIRM SECUNIA
webmediaexplorer -- webmedia_explorer	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Webmedia Explorer (webmex) 5.09 and 5.10 allow remote attackers to inject arbitrary web script or HTML via event handlers such as onmouseover in the (1) search or (2) tag parameters; (3) arbitrary invalid parameter names that are not properly handled when triggered on a column; (4) bookmark parameter in an edit action; or (5) email parameter in a remember action.	2009-06-17	4.3	CVE-2009-2107 BID BUGTRAQ SECUNIA MISC

[Back to top](#)**Low Vulnerabilities**

Primary	CVSS	Source & References
---------	------	---------------------

<b>Primary Vendor -- Product</b>	<b>Description</b>	<b>Published</b>	<b>CVSS Score</b>	<b>Source &amp; Patch Info</b>
apple -- iphone_os	Safari in Apple iPhone OS 1.0 through 2.2.1 and iPhone OS for iPod touch 1.1 through 2.2.1 does not properly clear the search history when it is cleared from the Settings application, which allows physically proximate attackers to obtain the search history.	2009-06-19	2.1	<a href="#">CVE-2009-1680</a> CONFIRM APPLE
cisco -- wrt160n	Cross-site request forgery (CSRF) vulnerability in Linksys WRT160N wireless router hardware 1 and firmware 1.02.2 allows remote attackers to hijack the authentication of other users for unspecified requests via unknown vectors, as demonstrated using administrator privileges and actions.	2009-06-15	0.0	<a href="#">CVE-2009-2073</a> XF VUPEN BID OSVDB SECUNIA MISC
drupal -- nodequeue	Cross-site scripting (XSS) vulnerability in Nodequeue 5.x before 5.x-2.7 and 6.x before 6.x-2.2, a module for Drupal, allows remote authenticated users with administer taxonomy permissions to inject arbitrary web script or HTML via vocabulary names.	2009-06-16	3.5	<a href="#">CVE-2009-2074</a> CONFIRM CONFIRM CONFIRM
drupal -- taxonomy_manager	Cross-site scripting (XSS) vulnerability in the administrative page interface in Taxonomy manager 5.x before 5.x-1.2 and 6.x before 6.x-1.1, a module for Drupal, allows remote authenticated users, with administer taxonomy privileges or the ability to use free tagging to add taxonomy terms, to inject arbitrary web script or HTML via (1) vocabulary names, (2) synonyms, and (3) term names.	2009-06-16	3.5	<a href="#">CVE-2009-2079</a> CONFIRM CONFIRM CONFIRM
mattias_hutterer -- taxonomy_manager	Cross-site scripting (XSS) vulnerability in the term data detail page in Taxonomy manager 5.x before 5.x-1.2, a module for Drupal, allows remote authenticated users, with administer taxonomy privileges or the ability to use free tagging to add taxonomy terms, to inject arbitrary web script or HTML via "Parent and related terms."	2009-06-16	3.5	<a href="#">CVE-2009-2083</a> CONFIRM CONFIRM
skybluecanvas -- skybluecanvas	admin.php in SkyBlueCanvas 1.1 r237 allows remote authenticated administrators to obtain sensitive information via an invalid id parameter, which reveals the installation path in an error message.	2009-06-18	3.5	<a href="#">CVE-2009-2115</a> XF

[Back to top](#)

Last updated June 22, 2009

 Print This Document